State of California

SECRETARY OF STATE

APPROVAL OF USE OF *ELECTION SYSTEMS AND SOFTWARE* UNITY 3.0.1.1 VOTING SYSTEM

I, DEBRA BOWEN, Secretary of State of the State of California, do hereby certify that:

I. Election Systems and Software, Inc. of Omaha, Nebraska ("Vendor"), has requested approval for use in California elections of its UNITY 3.0.1.1 voting system comprised of AutoMARK Voter Assist Terminal (VAT), Hardware version 1.0 (A100) and 1.1 (A200) with Firmware version 1.1.2258, AutoMARK Information Management System (AIMS) version 1.2.18, Model 100 Optical Scan Precinct Counter, Hardware version 1.3 with Firmware version 5.2.1.0, Model 650 Central Ballot Counter, Hardware version 1.1 with Firmware version 2.1.0.0, Election Data Manager (EDM), version 7.4.4.0, ES&S Image Manager (ESSIM), version 7.4.2.0, Hardware Program Manager (HPM), version 5.2.4.0, Election Reporting Manager (ERM), version 7.1.2.1, and Audit Manager, version 7.3.0.0, submitted on or about October 9, 2007.

II. The voting system described above has been federally qualified as evidenced by federal Independent Testing Authority reports and the assigned NASED Number # N-2-02-22-22-006 (2002), dated August 31, 2006.

III. The request for approval of the voting system as described in Paragraph 1, was considered at a public hearing held February 23, 2008, at Sacramento, California.

IV. STATE TESTING RESULTS

1. I, as Secretary of State, tasked Freeman, Craft, McGregor Group (FCMG) to perform "Red Team" analysis (penetration testing) of the ES&S Unity 3.0.1.1 Voting System with the goal of compromising the security of the voting system.

2. The Red Team demonstrated that several components of the voting system are vulnerable to attack, as illustrated by the vulnerabilities and attacks described below.

3. The Red Team found that the wire seal on the front panel of an M100 Tabulator, provided by ES&S, can be bypassed if it is not tightened correctly, providing a vector of attack on the PCMCIA cards inside.

4. The Red Team found that PCMCIA cards used by M100 Tabulators may be exchanged at the precinct during an election to implement ballot box stuffing attacks in favor of particular candidates, an exploit that is difficult to detect without examining the audit logs.

5. The Red Team found that all data on the PCMCIA card is unencrypted and can be viewed using commonly available programs. This enables a potential attacker to analyze the data on the card and develop strategies to defeat the embedded security mechanisms.

6. The Red Team identified an exploit that enables an attacker to gain unauthorized access to the Election Reporting Manager (ERM), enabling the attacker to manually add or remove votes from the official vote totals in a few seconds, tampering that, if executed properly, could only be detected by analyzing audit logs.

7. The Red Team found that the Zip disk containing the Model 650 tabulation results may be modified while it is transported to the Election Reporting Manager, which would process the modified vote totals without questioning their validity.

8. The Red Team found that an attacker with unauthorized access can gain complete access to the Audit Manager database by cracking the password, and upon gaining access, change records, create or remove login credentials for the Audit Manager, EDM, or ESSIM and delete audit log entries to make detection of the attack difficult.

9. The Red Team found that an attacker with unauthorized access to the Microsoft SQL Server database used by the AutoMARK Information Management System (AIMS) could write modified ballot definition files data to the Compact Flash card used by the AutoMARK Voter Assist Terminal (VAT), causing a vote cast with the audio ballot feature for one candidate to be marked as a vote for another candidate.

10. The Red Team found that an attacker with unauthorized access to the Microsoft SQL Server database used by the AutoMARK Information Management System (AIMS) could configure an AutoMARK VAT to display one candidate name on the screen while the audio ballot identified a different candidate.

11. The Red Team found that an attacker with physical access to the system and the appropriate expertise could obtain the password for accessing the Hardware Programming Manager (HPM) and Election Reporting Manager (ERM) in a few minutes.

12. The Red Team found that an attacker with unauthorized access working with a computer systems expert could disable the access control system for the Hardware Programming Manager (HPM) and the Election Reporting Manager (ERM) in a few

minutes, exposing these central components of the voting system to uncontrolled access, a serious breach of voting system security.

13. The Red Team also found that an attacker with unauthorized access could, rather than disabling the access control system for the HPM and ERM, selectively grant (or deny) any individual the right to access the HPM and ERM.

14. The Red Team found that an individual with sufficient expertise can pick the locks located in the front of the AutoMARK Voter Assist Terminal (VAT), the M100 Tabulator and the M650, with the time required by the Red Team to pick the locks ranging from five seconds to one minute.

15. The Red Team found that, while many of the vulnerabilities it identified can be partially mitigated by adopting various security policies and procedures, some of the vulnerabilities are due to system design and may, therefore, require hardware and/or software upgrades or re-design.

16. I, as Secretary of State, tasked atsec information security corporation, working under contract to Freeman, Craft, McGregor Group (FCMG), to conduct an analysis of the source code of the ES&S Unity 3.0.1.1 Voting System, with the goal of assessing the security and integrity of the system, and in particular, on identifying any security vulnerabilities that could be exploited to alter vote recording, vote results, or critical election data such as audit logs, or to conduct a "denial of service" attack on the voting system.

17. The Source Code Reviewers found that the M100 precinct ballot counters run code supplied on the election definition memory cards without effective measures to ensure the integrity and authenticity of this code. As a result, there is little assurance that the systems will actually be running the reviewed and authorized code at election time.

18. The Source Code Reviewers found that the system as a whole fails to provide strong Identification and Authentication for access control, with some components having no access controls at all, while components that restrict access by requiring a User ID, a password, or a User ID/password pair have the login credentials either hard coded in the source code, stored in clear text in a database, or at best, scrambled with extremely weak algorithms that do not prevent credentials from being discovered, potentially exposing all components in the system to unauthorized access.

19. The Source Code Reviewers found that election data is transferred among components of the Unity System via removable media devices, either in plain text, stored with simple checksum values, obfuscated with extremely weak algorithms, or at best encrypted with symmetric algorithms, allowing election data to be maliciously modified by a component of the Unity System or during the transition

of the media from one component to the other, but yet still be treated as valid by other Unity System components.

20. The Source Code Reviewers found that Unity version 3.0.1.1 fails to provide reliable accountability for its audit log, which are kept either in databases or log files, unprotected by any kind of tamper-detection mechanism, rendering the audit log susceptible to undetected tampering.

21. The Source Code Reviewers found that, because the developers generally assumed that input data will be supplied in the correct expected format, there was little validation checking of data, leading to potentially exploitable vulnerabilities.

22. The Source Code Reviewers concluded that, due to the multiple vulnerabilities in the code of the ES&S Unity 3.0.1.1 Voting System, the system's security depends on its secure use, which assumes that all parties involved in developing, maintaining, distributing, deploying and using the Unity system must be trustworthy, an assumption the reviewers equated to an unsupportable assumption that there are no threats to the system.

V. Election Systems and Software, Inc.'s UNITY 3.0.1.1 voting system as described in Paragraph 1, is hereby approved for use subject to the following terms and conditions:

1. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the Vendor and approved by the Secretary of State.

2. Prior to sale or use of the system in California, the Vendor must provide to all jurisdictions the revised version of its Use Procedures, entitled "California Election Procedures, May 2008" submitted by the Vendor on May 14, 2008, which the Secretary of State hereby approves. The revised Use Procedures address issues identified in the functional, source code, red team and accessibility testing reports from the state testing of the voting system. Compliance with the Use Procedures by the Vendor and jurisdictions is a condition of the approval of this voting system. Compliance with all requirements set forth in the Use Procedures is mandatory, whether or not a particular requirement is identified in this Approval document.

3. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy or efficiency of the voting systems sufficient to require a re-examination and approval.

4. Before any use in the November 4, 2008, General Election, jurisdictions must reformat all hard disk drives and reinstall the operating system, where applicable, before installing software and firmware on all election management system servers and workstations, voting devices and hardware components of the voting system. Jurisdictions must install voting system application software using the currently

approved version obtained directly from the federal testing laboratory or the Secretary of State.

5. The Vendor and jurisdictions must implement the specifications for the hardware and operating system platform for all applicable components of the voting system, as set forth on pages 47 and 48 of the Use Procedures. The Vendor and jurisdictions must comply with the requirements for "hardening" the configuration of that platform, as set forth in Appendix F, pages 803 through 807 of the Use Procedures, including, but not limited to:
   - BIOS configuration;
   - Essential services that are required and non-essential services that must be disabled;
   - Essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
   - Audit logging configuration;
   - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
   - Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
   - Specifications for the installation, configuration and use of all utilities and software applications necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.), as set forth on page 9 of the Use Procedures under the heading "COTs Overview."

6. Immediately after any repair or modification of any voting system component that requires opening the housing, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.

7. No network connections to any device not directly used and necessary for voting system functions may be established. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.

8. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.

9. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and one audit log from each device. Each poll worker must sign every copy. One copy of the vote results from each device must be publicly posted outside the polling place. The second copy, along with the audit

log, must be included with the official election material that is returned to the jurisdiction headquarters on election night.

10. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.

11. Poll workers are not permitted to participate in any post-election manual count auditing of precinct results from a precinct in which they were a poll worker.

12. Elections officials must comply with additional post-election manual count auditing requirements as set forth by the Secretary of State in the document entitled "Post-Election Manual Tally Requirements" and any successor document. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the Vendor. Elections officials are required to conduct the audits and the Vendor is required to reimburse the jurisdiction.

13. Each polling place must be equipped with a method or log to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:
    - Date and time of occurrence;
    - Voter involved, if any;
    - Equipment involved;
    - Brief description of occurrence;
    - Actions taken to resolve issue, if any; and
    - Elections official(s) who observed and/or recorded the event.

14. All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the elections official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.

15. Training of poll workers must include each of the topics identified on pages 594 and 595 of the Use Procedures.

16. Elections officials must develop appropriate security procedures for use when representatives of qualified political parties and bona fide associations of citizens and media associations, pursuant to their rights under Elections Code section 15004.

17. All voters voting on paper ballots in a polling place must be provided a privacy sleeve for their ballot and instructed on its use in accordance with Elections Code section 14272.

18. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with

voting equipment or altering vote results constitutes a felony, punishable by imprisonment.

19. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
    - The chief elections official of the jurisdiction must be notified immediately;
    - The equipment must be removed from service immediately and replaced if possible;
    - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, as part of the official canvass. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;
    - Any memory card containing data from that device must be secured and retained for the full election retention period;
    - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period; and
    - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.

20. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
    - The chief elections official of the jurisdiction must be notified immediately;
    - The equipment must be removed from service immediately and replaced as soon as possible;
    - Any votes cast on the device prior to its removal from service must be subject to a 100% manual tally, by the process described in Elections Code section 15360, over and above the normal manual tally conducted during the official canvass as defined in Elections Code section 336.5. Notice to the public of this manual tally may be combined with the notice required by any other manual tally required in this order or by Elections Code section 15360;
    - Any memory card containing data from that device must be secured and retained for the full election retention period;
    - An image of all device software and firmware must be stored on write-once media and retained securely for the full election retention period;
    - The Vendor or jurisdiction shall provide an analysis of the cause of the failure;
    - Upon request by the Secretary of State, the Vendor or jurisdiction shall retain the device for a reasonable period of time to permit forensic analysis; and
    - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing

laboratory or the Secretary of State before the equipment is placed back into service.

21. The Secretary of State reserves the right, with reasonable notice to the Vendor and to the jurisdictions using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.

22. Any jurisdiction using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel Plan.

23. The Vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the Vendor, provided that the Secretary of State first commits to the Vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the Vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the Vendor. The voting system shall not be installed in any California jurisdiction until the Vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be borne by the Vendor.

24. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, test voting equipment.

25. By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of the California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.

26. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and

federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.

27. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.

28. The Vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.

29. In addition to depositing the source code in an approved escrow facility, the Vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.

30. The Vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The Vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.

IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 30th day of June, 2008.

THE GREAT SEAL OF THE STATE OF CALIFORNIA
EUREKA

Debra Bowen

DEBRA BOWEN
Secretary of State